

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-31129

(43)公開日 平成11年(1999) 2 月 2 日

(51)Int.Cl. ⁶	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 A
13/00	3 5 1	13/00 3 5 1 E
17/30		15/40 3 1 0 F
H 0 4 L 9/32		3 2 0 B
		H 0 4 L 9/00 6 7 3 C
審査請求 未請求 請求項の数8 O L (全 11 頁)		

(21)出願番号 特願平9-188524

(22)出願日 平成9年(1997) 7 月14日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 中島 充

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 門間 仁

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

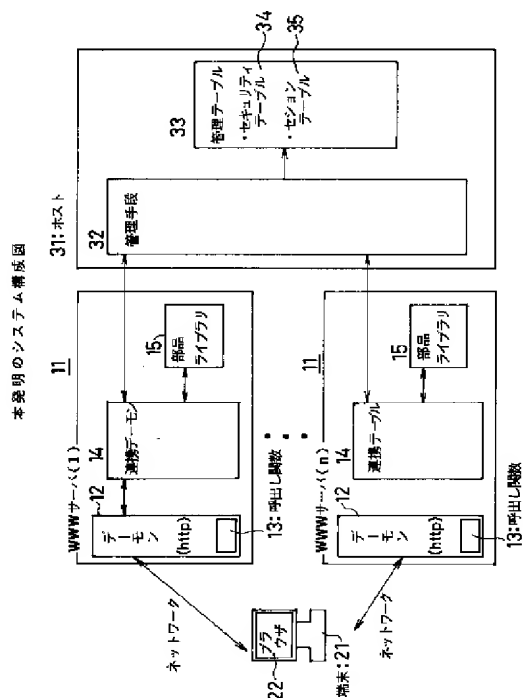
(74)代理人 弁理士 岡田 守弘

(54)【発明の名称】 複数WWWサーバ連携システム

(57)【要約】

【課題】 本発明は、複数WWWサーバ連携システムに関し、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセッションIDをもとに複数ページや異なる複数のWWWサーバに渡ってアクセスを可能にするシステムを実現することを目的とする。

【解決手段】 ホストは複数のいずれかのWWWサーバから通知されたブラウザからのHTML文書を解析し、セッションIDが付加されていなかったときにユーザ情報の入力要求を上記WWWサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッションIDを生成し、ふたたびWWWサーバを介してセッションIDの埋め込んだHTML文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すように構成する。



【特許請求の範囲】

【請求項 1】ブラウザから受信した HTML 文書をホストに通知、およびホストから通知を受けたセッション ID を HTML 文書に埋め込んでブラウザに送信あるいはホストから通知を受けたセッション ID を埋め込んだ HTML 文書をブラウザに送信する複数の WWW サーバ等を備えたネットワークシステムにおいて、

上記ホストは上記複数のいずれかの WWW サーバから通知されたブラウザからの HTML 文書を解析し、セッション ID が付加されていなかったときにユーザ情報の入力要求を上記 WWW サーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッション ID を生成し、ふたたび WWW サーバを介してセッション ID の埋め込んだ HTML 文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すことを特徴とする複数 WWW サーバ連携システム。

【請求項 2】上記セッション ID を HTML 文書に埋め込む際に、URL 上に表示しないようにセッション ID を HTML 文書上に埋め込み、セッション ID を不可視としたことを特徴とする請求項 1 記載の複数 WWW サーバ連携システム。

【請求項 3】上記 WWW サーバに、ブラウザとの間で HTML 文書の送受信を行うデーモン中に連携デーモンを呼び出す呼び出し関数と、この呼び出し関数から呼び出されたときにブラウザから受信した HTML 文書をホストに通知、およびホストから通知を受けたセッション ID を HTML 文書に埋め込んでブラウザに送信あるいはホストから通知を受けたセッション ID を埋め込んだ HTML 文書をブラウザに送信する連携デーモンとを備えたことを特徴とする請求項 1 あるいは請求項 2 記載の複数 WWW サーバ連携システム。

【請求項 4】上記 WWW サーバに、上記連携デーモンから依頼を受けた処理を実行する部品ライブラリを備えたことを特徴とする請求項 3 記載の複数 WWW サーバ連携システム。

【請求項 5】上記有効時間情報として、上記ユーザ情報に対応づけて認証有効時間を設定したことを特徴とする請求項 1 ないし請求項 4 記載のいずれかの複数 WWW サーバ連携システム。

【請求項 6】上記 WWW サーバ上の HTML 文書毎あるいは複数の HTML 文書をまとめたディレクトリ毎に認証の有無を設定し、認証有のときにのみ上記呼び出し関数が上記連携デーモンを呼び出すことを特徴とする請求項 3 ないし請求項 5 記載のいずれかの複数 WWW サーバ連携システム。

【請求項 7】ブラウザから受信した HTML 文書をホストに通知、およびホストから通知を受けたセッション ID を HTML 文書に埋め込んでブラウザに送信あるいはホストから通知を受けたセッション ID を埋め込んだ HTML

L 文書をブラウザに送信する WWW サーバ上で動作するプログラムを格納した記録媒体。

【請求項 8】複数のいずれかの WWW サーバから通知されたブラウザからの HTML 文書を解析し、セッション ID が付加されていなかったときにユーザ情報の入力要求を WWW サーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッション ID を生成し、ふたたび WWW サーバを介してセッション ID の埋め込んだ HTML 文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すホスト上で動作するプログラムを格納した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数 WWW サーバが連携する複数 WWW サーバ連携システムに関するものである。

【0002】

【従来の技術】従来、WWW サーバの通信プロトコルである HTTP (Hyper Text Transfer Protocol) のセッションは、ブラウザがページを要求するときに設定し、サーバがそのページを送信すると切断されてしまう。このようにセッションは、ページごとに切れてしまい、次のページ（画面）にアクセスした場合には、全く別のセッションになる。

【0003】そのため、利用者の認証が必要なページに対しては、ページ単位に利用者の認証を行うようにしていた。

【0004】

【発明が解決しようとする課題】上述したように従来の認証は、ブラウザから WWW サーバのページをアクセスする毎に利用者認証を要求し、ブラウザがその認証に必要な情報（ユーザ ID、パスワードなどの情報）を入力して送信しサーバが認証を行うという面倒な操作が認証に必要なページ毎に発生してしまうという問題があった。

【0005】また、ブラウザから同一機能の他の WWW サーバをアクセスした場合には、当然に認証が必要なページ毎にその認証に必要な情報を入力して送信しサーバが認証を行わなければならないという問題もあった。

【0006】本発明は、これらの問題を解決するため、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセッション ID をもとに複数ページや異なる複数の WWW サーバに渡ってアクセスを可能にするシステムを実現することを目的としている。

【0007】

【課題を解決するための手段】図 1 を参照して課題を解決するための手段を説明する。図 1 において、WWW サーバ 11 は、ブラウザ 22 から受信した HTML 文書をホスト 31 に通知したり、ホスト 31 から通知を受けた

セッションIDをHTML文書に埋め込んでブラウザ22に送信あるいはホスト31から通知を受けたセッションIDを埋め込んだHTML文書をブラウザ22に送信したりなどするものであって、デーモン12、連携デーモン14、部品ライブラリ15などから構成されるものである。

【0008】デーモン12は、データをブラウザ22との間でネットワークを介して送受信するものであって、ここでは、呼び出し関数13などを持つものである。呼び出し関数13は、ブラウザ22からHTML文書を受信したときに連携デーモン14を呼び出すものである。

【0009】連携デーモン14は、呼び出し関数13から呼び出され、デーモン12が受信したHTML文書をホスト21に通知したり、ホスト31から通知されたHTML文書をデーモン12に通知したり、部品ライブラリ14を呼び出して所定処理を依頼したりなどするものである。

【0010】部品ライブラリ15は、連携デーモン14から依頼を受けた各種処理を行う部品（プログラム）である。ブラウザ22は、ネットワークを介してWWWサーバ11と接続して当該WWWサーバ11から受信したHTML文書を画面に表示したり、画面上で文書／イメージが選択されたときに該当するHTML文書などをWWWサーバ11に送信したりなどするものである。

【0011】ホスト31は、WWWサーバ11を構成する連携デーモン14から通知されたHTML文書をもとに各種処理を行ったり、データを連携デーモン14経由でブラウザ22に送信したりなどするものである。

【0012】次に、動作を説明する。WWWサーバ11がブラウザ22から受信したHTML文書をホスト31に通知し、ホスト31が通知されたブラウザ22からのHTML文書を解析し、セッションIDが付加されていなかったときにユーザ情報の入力要求をWWWサーバ11を介してブラウザ22に送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッションIDを生成し、ふたたびWWWサーバ11を介してセッションIDの埋め込んだHTML文書をブラウザ22に送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すようにしている。

【0013】この際、セッションIDをHTML文書に埋め込むときに、URL上に表示しないようにセッションIDをHTML文書に埋め込み、セッションIDを不可視とするようにしている。

【0014】また、WWWサーバ11に、ブラウザ22との間でHTML文書などの送受信を行うデーモン12中に連携デーモン14を呼び出す呼び出し関数13を設け、呼び出し関数13から呼び出された連携デーモン14がブラウザ22から受信したHTML文書をホスト31に通知し、ホスト31から通知を受けたセッションIDをHTML文書に埋め込んでデーモン12を介してモブ

ブラウザ22に送信あるいはホスト31から通知を受けたセッションIDを埋め込んだHTML文書をデーモン12を介してブラウザ22に送信するようにしている。

【0015】また、WWWサーバ11に、連携デーモン14から依頼を受けた処理を実行する部品ライブラリ15を設け、当該部品ライブラリ15に各種処理を依頼するようにしている。

【0016】また、ホスト31が有効時間情報として、ユーザ情報に対応づけて認証有効時間を設定し、セッションIDの有効性を判断するようにしている。また、WWWサーバ11上のHTML文書毎に認証の有無を設定し、認証の有のときにのみ呼び出し関数13が連携デーモン14を呼び出すようにしている。

【0017】従って、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセッションIDをもとに複数ページや異なる複数のWWWサーバ11に渡ってアクセスすることが可能となる。

【0018】

【発明の実施の形態】次に、図1から図8を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0019】図1は、本発明のシステム構成図を示す。図1において、WWWサーバ11は、ブラウザ22からネットワークを介して受信したHTML文書をホスト31に通知したり、ホスト31から通知を受けたセッションIDをHTML文書に埋め込んでネットワークを介してブラウザ22に送信あるいはホスト31から通知を受けたセッションIDを埋め込んだHTML文書をネットワークを介してブラウザ22に送信したりなどするものであって、デーモン12、連携デーモン14、部品ライブラリ15などから構成されるものである。このWWWサーバ11は、例えば後述する図2中のWWWサーバと記載した処理を行う。ここで、HTML文書はブラウザの画面上に文書やイメージを表示するようにHTML言語で記述した文書であり、他にURL（アドレス）およびヘッダ情報（HTTPプロトコルで使用する情報）がある。

【0020】デーモン（http）12は、HTTPプロトコルを使用してネットワークを介してデータ（URL、html文書など）をブラウザ22との間で授受するものであって、ここでは、呼び出し関数13などを持つものである。

【0021】呼び出し関数13は、ブラウザ22からHTML文書を受信したときに連携デーモン14を呼び出すものである。連携デーモン14は、呼び出し関数13から呼び出され、デーモン12が受信したHTML文書をホスト21に通知したり、ホスト31から通知されたHTML文書をデーモン12に通知したり、部品ライブラリ14を呼び出して所定処理を依頼したりなどするものであって、例えば後述する図2中に連携デーモンと記載した処理を行うものである。

10

20

30

40

50

【0022】部品ライブラリ15は、連携デーモン14から依頼を受けた各種処理を行う部品であって、例えば後述する図2中に部品と記載した処理を行うものである。端末21は、ネットワークを介してWWWサーバ11と接続し、HTTPプロトコルを用いてデータの授受を行うものであって、ここでは、ブラウザ22などから構成されるものである。

【0023】ブラウザ22は、ネットワークを介してWWWサーバ11と接続して当該WWWサーバ11から受信したHTML文書を画面に表示したり、画面上で文書／イメージが選択されたときに該当するHTML文書などをWWWサーバ11に送信したりなどするものであって、ネットエスケープ（製品名）などの汎用のブラウザ（HTML文書を表示などするプログラム）である。

【0024】ホスト31は、WWWサーバ11を構成する連携デーモン14から通知されたHTML文書をもとに各種処理を行ったり、データを連携デーモン14経由でブラウザ22に送信したりなどするものであって、ここでは、管理手段32および管理テーブル33などから構成されるものであり、後述する図2のホストと記載した各種処理を行うものである。

【0025】管理手段31は、管理テーブル32を参照して認証を行ったり、認証OKのときにデータをブラウザ22に向けて送信したりなどするものである。管理テーブル32は、各種管理情報を登録して管理するテーブルであって、ここでは、セキュリティテーブル34およびセッションテーブル35などから構成されるものである。

【0026】セキュリティテーブル34は、HTML文書のセキュリティ情報を管理するものであって、例えば後述する図3に示すような情報を管理するものである。セッションテーブル35は、セッションIDの認証有効時間を管理するものであって、ここでは、例えば後述する図4に示すような情報を管理するものである。

【0027】次に、図2に示す順番に従い、図1の構成の動作を詳細に説明する。図2は、本発明の動作説明図を示す。ここで、ブラウザ、WWWサーバ、およびホストは、図1のブラウザ22、WWWサーバ11、およびホスト31にそれぞれ対応するものである。

【0028】図2において、S1は、参照するURLの指定を行う。これは、ブラウザ22が参照するURL（アドレス）の指定に対応して、当該URLをWWWサーバ11に送信する。

【0029】S2は、WWWサーバ11がURLを受け取る（受信する）。S3は、URLの解析を行う。S4は、S3のURLの解析の結果、プラグイン関数の呼び出しが判別する。YESの場合には、本発明に係る以下の処理を実行し、S7で呼び出し関数13が連携デーモン14を呼び出し、S8で常駐デーモン（連携デーモン）への引渡を行い、S9で認証要求をホスト31に通

知し、S10に進む。一方、S4のNOの場合には、プラグイン関数の呼出しがないと判明したので、S5でhtml文書の送出手続きを行い、S8でブラウザ22がhtml文書を画面上に表示する。

【0030】以上のS1ないしS9によって、ブラウザ22が参照するURLをWWWサーバ11に送信し、WWWサーバ11のデーモン（http）12がURLを受信してプラグイン関数呼出しが必要か否かを判別し、YESの場合（必要な場合）には連携デーモン14を呼び出し、認証要求をホスト31に通知することが可能となり、一方、NOの場合（必要でない場合）には従来通り、URLに対応するhtml文書をブラウザ22に送信してブラウザ22がhtml文書を画面上に表示することが可能となる。

【0031】S10は、ホスト31が連携デーモン14からの認証要求を受け取る。S11は、URLの解析を行う。S12は、認証に必要なURLかどうかの判定を行う。これは、URLで指定されたhtml文書が認証を必要とするものであるか否かについて、後述する図2のセキュリティテーブル34を参照して判定する。認証が必要な場合には、S15に進む。一方、認証が不要の場合には、S13でhtml文書をWWWサーバ11を介してブラウザ22に送信し、S14でブラウザ22が受信したhtml文書について画面上に表示する。

【0032】S15は、S12で認証が必要と判明したので、指定されたURLの認証範囲の取り出しを行う。S16は、セッションIDが付加されているか判別する。これは、S15でブラウザ22から受信したURLの認証範囲にセッションIDが付加されているか判別する（既に以前にセッションIDが付加されているか判別する）。YESの場合には、既に以前にセッションIDがS17ないしS37によってセットされていたと判明したので、S41に進む。一方、NOの場合には、セッションIDがセット（付加）されていないと判明したので、S17ないしS32によってセッションIDの付加を行う。

【0033】S17は、S16でセッションIDが付加されていないと判明したので、ID、パスワード画面（java）の送出要求をWWWサーバ11に通知する。S18は、WWWサーバ11の連携デーモン14が受け付ける。

【0034】S19は、S18で受け付けた連携デーモン14から部品ライブラリ15中の部品がID、パスワード入力用html（java、html）を送出する。S20は、S19で送出されたパスワード入力用html（java）の表示をブラウザ22上で行う。

【0035】S21は、S20で表示されたパスワード入力用画面上でID、パスワード入力する。例えば後述する図5のパスワード／ID入力画面上でユーザがユーザID、パスワードを入力し、STARTボタンを押下する。

【0036】S22は、ID、パスワードを暗号化(java)してWWWサーバ11に送信する。S23は、受取情報の送出(再暗号化)を行う。これは、WWWサーバ11がS22で送信されたID、パスワードの暗号化した情報を受け取り、この情報を再暗号化してサーバ11に送信する。

【0037】S24は、サーバ31がS23で送信された情報を受け取り、復号化する。S25は、S24で復号化したID、パスワードを取り出す。S26は、ID、パスワードの検索を行う。これは、例えば後述する図4のセッションテーブル35中のID(ユーザID、パスワード)の検索を行い、一致するものがあるか判別する。OKの場合には、S29に進む。NGの場合には、一致するID、パスワードが登録されていないとエラーと判明したので、WWWサーバ11に指示してS27でエラー表示用htmlを送信し、S28でブラウザ22が受信したエラー表示htmlによって画面上にエラー表示を行う。

【0038】S29は、S26でID、パスワードを検索して一致するものと判明したので、更に認証範囲の判定を行う。これは、図示外のユーザID毎の認証範囲の判定を行い、当該ユーザIDに認証権限が付与されているか判別する。OKの場合には、S30に進む。NGの場合には、ユーザIDに認証権限が付与されていないと判明したので、S27でエラー表示用htmlを送出し、S28でブラウザ22がエラー表示htmlを画面上に表示する。

【0039】S30は、S29のOKで認証権限がありと判明したので、セッションIDのセットを行う。セッションIDは、一意のIDであって、例えば後述する図4に示すように、現時刻の年月日時分秒ミリ秒からなる一意のセッションIDを、図4のセッションテーブル35中のセッションIDの該当する欄にセットして記憶する。

【0040】S31は、認証保証時間のセットを行う。これは、後述する図4のセッションテーブル35の認証有効時間を取り出して現時刻に加算して認証満了時間を求めて図4の当該認証満了時間の欄にセットする。

【0041】S32は、セッションIDの送出を行う。S33は、WWWサーバ11の連携デーモン14がS32で送出されたセッションIDを受け取る。

【0042】S34は、部品が指定されたURLにセッションIDを付加する。これは、例えば後述する図8の(a)の指定されたURLにセッションIDを付加し、図8の(b)のURL(セッションID付加)を生成する。

【0043】S35は、付加URLを固定のURLに再編集する。これは、S34でセッションIDを付加した図8の(b)のURL(セッションID付加)について、固定のURLとして、図8の(c)のURL(cgi付加)を生成、即ち、システムで固定のデータを図示のように付加し、元の正しいセッションIDをhtml文書中

に埋め込み、URL(cgi付加)が明示的に表示されてもセッションIDが表示されないようにして他人に見えないようにする(不可視にする)。

【0044】S36は、html文書を送出する。S37は、S36で送出されたhtml文書をブラウザ22が画面上に表示する。この際、URL(cgi)が表示されるが、当該URLにはシステムで固定のcgi(例えば××××.cgi)が表示されるのみで、正しいセッションIDは不可視とし、html文書中に埋め込むようにしている。そして、S1に戻り繰り返す。

【0045】また、S41は、S16でセッションIDが付加されていると判明したので、セッションIDの検索を行う。これは、セッションIDについて、図4のセッションテーブル35に登録されているか判別する。OKの場合には、S42に進む。NGの場合には、セッションIDがセッションテーブル35に登録されていないと判明したので、既述したS17以降の処理を行い、セッションIDの再登録を行う。

【0046】S42は、セッションIDの有効範囲内か判別する。これは、後述する図4のセッションテーブル35を参照して該当するセッションIDのエントリ中の認証満了時間内に、現時刻があつて当該セッションIDが有効か判別する。OKの場合には、既述したS33以降の処理を実行する。NGの場合には、セッションIDがセッションテーブル35に登録されているが有効時間範囲内でないと判明したので、既述したS17以降の処理を行い、セッションIDの再登録を行う。

【0047】以上によって、URL解析を行い、認証が必要なURLの場合には、セッションIDが付加されていないときにID、パスワード入力画面をブラウザ22に送信して表示させ、入力されたID、パスワードが正しいときに一意のセッションIDを付加し、一方、セッションIDが付加されていたときに当該セッションIDが有効時間範囲内のときにセッションIDをhtml文書中に不可視に付加してブラウザ22に送信し、また、セッションIDが付加されていても有効時間範囲内でないときはID、パスワード入力画面をブラウザ22に送信して表示させ、入力されたID、パスワードが正しいときに一意のセッションIDを再付加することにより、html文書中に不可視に埋め込んだセッションIDをもとに、有効時間範囲内についてブラウザ22とサーバ31とが任意のWWWサーバ11を経由して送受信することが可能となる。以下順次詳細に説明する。

【0048】図3は、本発明のセキュリティテーブル例を示す。これは、SOP、TYPE、URLを対応づけて登録したものである。ここで、SOPは、図示のように

- ・001：サービス種別を表し
- ・PUB：公開を表し
- ・BAS：基本を表す。

【0049】また、TYPEは、図示のように

- ・00：認証（有料）を表す。
- ・01：認証（無料）を表す。

【0050】

- ・BS：基本を表す。
- ・PUB：公開を表す。

また、URLは図示のようにディレクトリ、html文書をつなげたものである。

【0051】以上のように、セキュリティテーブル34によって、html文書毎にSOP、TYPEできまるセキュリティを登録して管理するようにしたものである。図4は、本発明のセッションテーブル例を示す。このセッションテーブル35は、図示のように、ユーザID、パスワードに対応づけて認証有効時間、パトロール時間、タイム監視時間を予め登録しておき、実際にブラウザ22から認証が必要なURLをホスト31が最初に受信したときに一意のセッションID（図示のように現時刻の年月日時分秒ミリ秒で決まる一意のセッションID）を付加して当該セッションテーブル35のセッションIDの欄にセットして登録および現時刻に認証有効時間を加算して求めた認証満了時間をセッションテーブル35の当該認証満了時間の欄にセットするものである。そして、セッションIDをhtml文書に不可視に埋め込んでホスト31とブラウザ22との間で任意のWWWサーバ11を経由して授受し、認証満了時間を経過するまでセッションIDを有効なものとして扱い、ホスト31がデータをブラウザ22に送信したりなどするようにしている。

【0052】また、セッションテーブル35中のパトロール時間は、当該セッションテーブル35中のエントリ中の認証満了時間を経過して不要なものがあるか否かをパトロールする時間間隔であって、無効なものは削除してメモリ容量を削減するためのものである。また、タイム監視時間は、各種タイマを監視する時間を設定するものである。

【0053】尚、セッションテーブル35中のID、パスワードは、図示外のオフラインでユーザIDおよびパスワードを登録したマスタDBに登録されたユーザID、パスワードのコピーである。

【0054】図5は、本発明のID／パスワード入力画面例を示す。これは、既述した図2のS20でブラウザ22の画面上に表示したID／パスワードの入力画面例であって、図示のように、ユーザID、パスワードを入力する領域を表示したものである。これらユーザIDおよびパスワードの入力領域に入力してSTARTボタンを押下すると、既述した図2のS22によって暗号化してWWWサーバ11に送出する。

【0055】図6は、本発明のID／パスワード認証フローチャートを示す。図6において、S51は、ID／パスワードがマスタDBに登録済か判別する。YESの場合には、S52で認証OKと判別する。NOの場合には、

は、図5のID／パスワード入力画面上で入力されたWWWサーバ11を経由してホスト31に通知されたID、パスワードがマスタDBに登録されないと判明したので、S53で認証NGと決定する。

【0056】図7は、本発明の認証範囲の判定フローチャートを示す。これは、既述した図3のセキュリティテーブル34に登録されたTYPEをもとに認証範囲を判定するフローチャートである。

【0057】図7において、S61は、URLで指定された図3のセキュリティテーブル34のTYPEの欄の値（00、01、BS、PUB）のいずれかを判別する。S62は、TYPEの欄の値（00、01、BS、PUB）によってそれぞれ認証OK／認証NGの判定を行う。

【0058】・TYPE＝00の場合には、S63で有料サービス資格有か判別し、YESのときにS64で認証OKと判定され、NOのときにS65で認証NGと判定される。

【0059】・TYPE＝01の場合には、S66で無料サービス資格有か判別し、YESのときにS67で認証OKと判定され、NOのときにS68で認証NGと判定される。

【0060】・TYPE＝BSの場合には、S69で認証OKと判定される。

・TYPE＝PUBの場合には、S70で認証OKと判定される。

図8は、本発明のURL／html文書例を示す。

【0061】図8の（a）は、URLの例を示す。ここでは、

URLは、http://www.fujitsu.co.jp
html文書は、当該html文書中に図示の
・HREF:URLデータを埋め込んだものである。

【0062】図8の（b）は、URL（セッションID付加）の例を示す。ここでは、

URL（セッションID付加）は、http://www.fujitsu.co.jp?END=yymddhhmmssxxx
html文書は、当該html文書中に図示の
・HREF:URL（セッションID）データを埋め込んだもの（不可視に埋め込んだもの）である。

このURL（セッションID付加）をそのままブラウザ22に送出すると、明示的に表示されてしまい、セッションIDが見えてしまうので、このままではブラウザ22に送出しない。

【0063】図8の（c）は、URL（cgi付加）の例を示す。ここでは、

URL（cgi付加）は、http://www.fujitsu.co.jp/xxxx.cgi
html文書は、当該html文書中に図示の
・HREF:URL（セッションID）データを埋め込んだもの（不可視に埋め込んだもの）である。

のURL (c g i 付加) をブラウザ 2 2 に送出しても、明示的に「・・・x x x x . c g i」が表示されるのみで、セッションID「yymdddhmmssxxx」が明示的に表示されることはなく、秘密に保持することが可能となる。

【0064】

【発明の効果】以上説明したように、本発明によれば、複数のいずれかのWWWサーバから通知されたブラウザからのHTML文書を解析し、セッションIDが付加されていなかったときにユーザ情報の入力要求をWWWサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッションIDを生成し、ふたたびWWWサーバを介してセッションIDの埋め込んだHTML文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許す構成を採用しているため、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセッションIDをもとに複数ページや異なる複数のWWWサーバに渡ってアクセスすることができる。このように不可視のセッションIDによって複数のWWWサーバに跨がったセッション管理を実現することが可能となった。

【図面の簡単な説明】

【図1】本発明のシステム構成図である。

*【図2】本発明の動作説明図である。

【図3】本発明のセキュリティテーブル例である。

【図4】本発明のセッションテーブル例である。

【図5】本発明のID/パスワード入力画面例である。

【図6】本発明のID/パスワード認証フローチャートである。

【図7】本発明の認証範囲の判定フローチャートである。

【図8】本発明のURL/h t m l 文書例である。

【符号の説明】

11：WWWサーバ

12：デーモン (h t t p)

13：呼出し関数

14：連携デーモン

15：部品ライブラリ

21：端末

22：ブラウザ

31：ホスト

32：管理手段

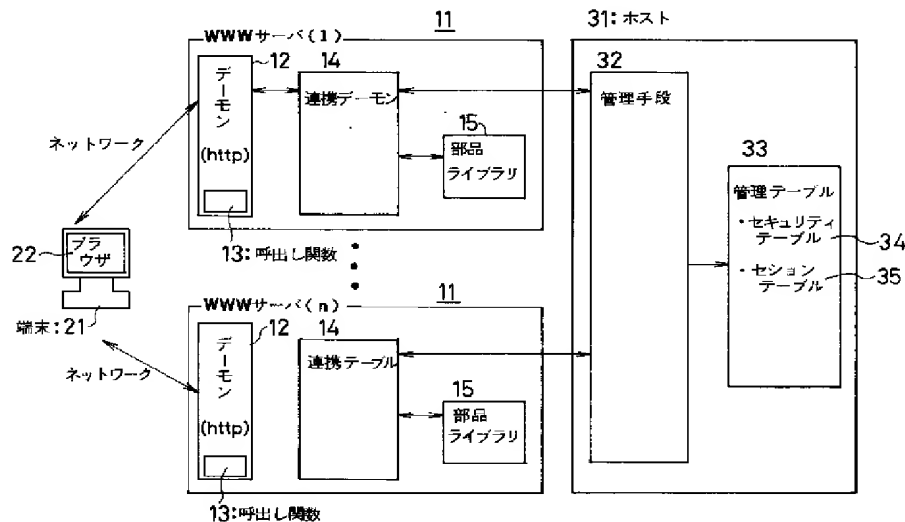
33：管理テーブル

34：セキュリティテーブル

35：セッションテーブル

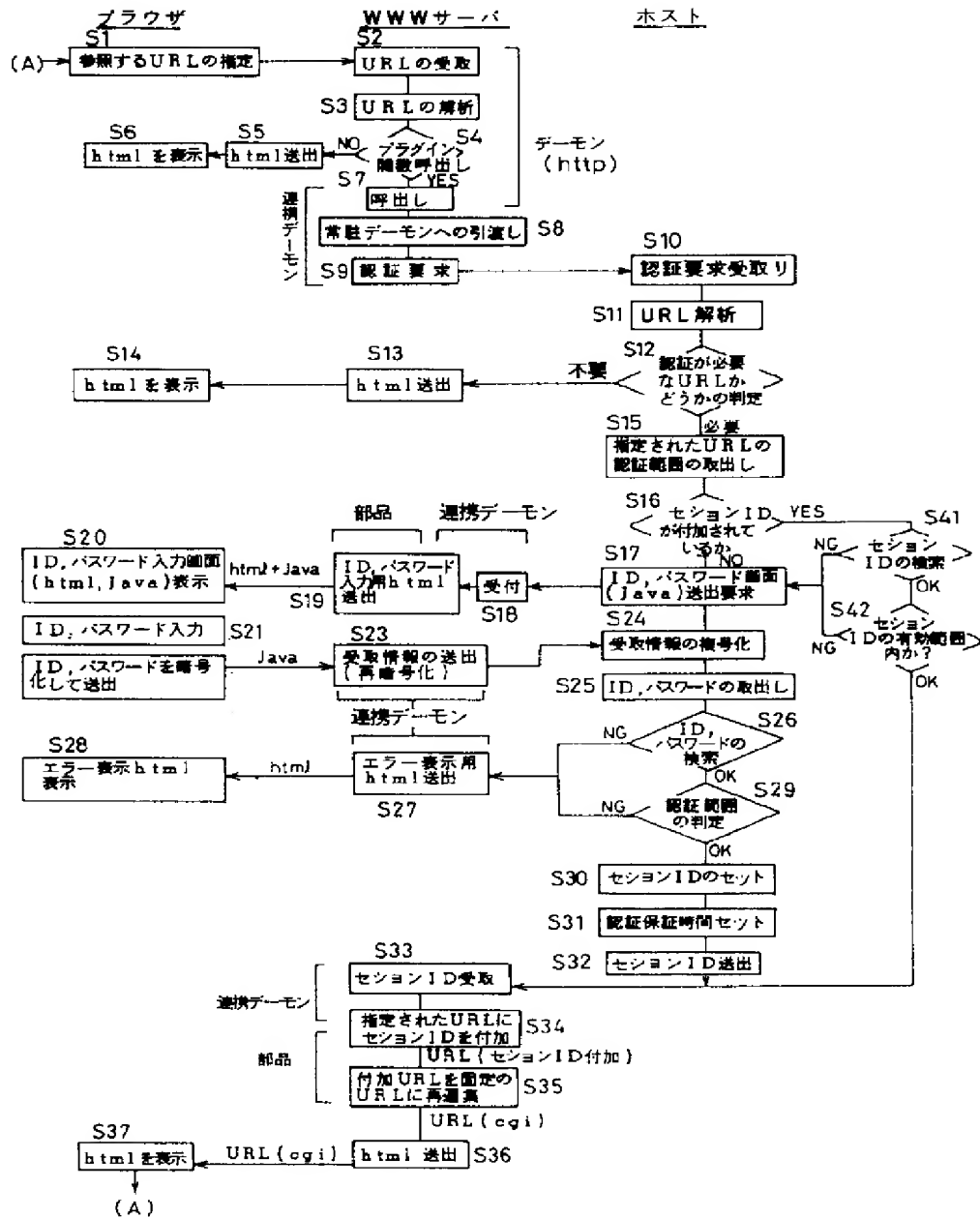
【図1】

本発明のシステム構成図



【図2】

本発明の動作説明図



【図 3】

本発明のセキュリティテーブル例

34

SOPT	TYPE	URL
001	00	/AAA/A.htm

001: サービス種別
 PUB: 公開
 BAS: 基本

00: 認証(有料)
 01: 認証(書類)
 BS: 基本
 PUB: 公開

/AAA/A.htm
 ディレクトリ htm文書

【図 5】

本発明のID/パスワード入力画面例

○ ○ ○ ○ ホームページ	
ユーザ ID	<input style="width: 100%;" type="text"/>
パスワード	<input style="width: 100%;" type="password"/>
<input type="button" value="START"/>	

【図 4】

本発明のセッションテーブル例

35

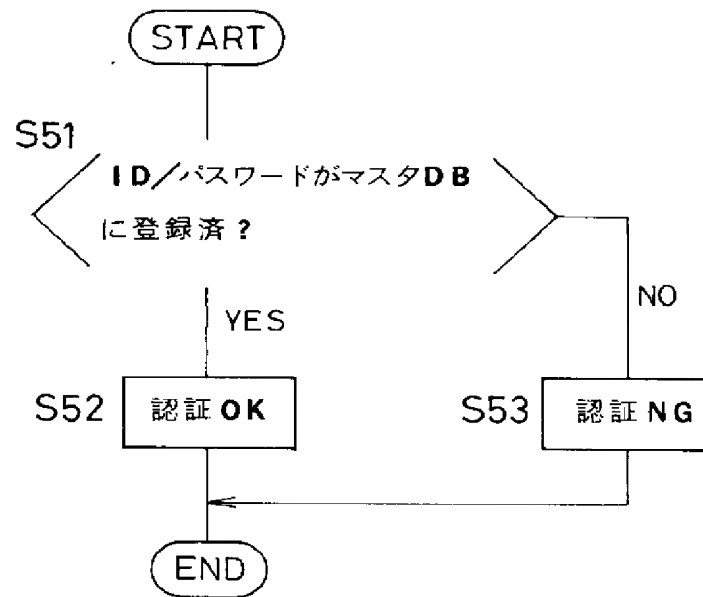
セッションID	ID	パスワード	認証有効時間 A+r	パトロール 時間 P+r	タイマ監視 間隔 Tsup	認証満了 時間 Tau+h
yymmddhhmmssxxx	A	XXX	003000	001000	001000	013000
			⋮			

マスタDBのコピー

セッションID yy mm dd hh mm ss xxx
 年 月 日 時 分 秒 ミリ秒

【図6】

本発明のID/パスワード認証フローチャート



【図8】

本発明のURL/html文書例

(a) URL

http://www.fujitsu.co.jp



(b) URL(セッションID付加)

http://www.fujitsu.co.jp?END=yyymmddhhmmssxxx

Labels for the URL components: URL, 制御記号 (Control Symbol), キーワード (Keyword), セッションID (Session ID). The session ID is further broken down into 年 (Year), 月 (Month), 日 (Day), 時 (Hour), 分 (Minute), 秒 (Second), and m秒 (Milliseconds).



(c) URL(cgi付加)

http://www.fujitsu.co.jp/xxx.cgi

システムで固定

html文書
HREF=URLデータ

html文書
HREF=URL(セッションID)データ

html文書
HREF=URL(セッションID)データ

【図 7】

本発明の認証範囲の判定フローチャート

